Bundesverband
Breitbandkommunikation e.V.

BREKO | Invalidenstraße 91 | 10115 Berlin

Per Mail: NIS2@bmi.bund.de
Bundesministerium des Innern und für Heimat
Referat CI 1 und Referat CI 3
11014 Berlin

BREKO Bundesverband
Breitbandkommunikation e.V.
Invalidenstraße 91
10115 Berlin

Tel.: +49 30 58580 418
kind@brekoverband.de

20.Oktober 2023

Stelliungnahme zum Diskussionspapier der BMI zu den wirtschaftsbezogenen Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutscland

Sehr geehrte Damen und Herren,

das Bundesministerium des Inneren und für Heimat (BMI) hat am 28.09.2023 ein „Diskussionspapier zur Umsetzung der NIS-2-Richtlinie in Deutschland“ zur Kommentierung versandt. Wir begrüßen sehr, dass das BMI mit dem Diskussionspapier zu einem frühen Zeitpunkt den Dialog mit der Wirtschaft sucht und bedanken uns für die Möglichkeit zur Abgabe einer Stellungnahme.

I. Einleitung

Der im Jahr 1999 gegründete Bundesverband Breitbandkomunikation (BREKO e.V.) vertritt die Interessen von knapp 480 Mitgliedsunternehmen, darunter über 240 Netzbetreibern, die vor allem lokal und regional echte Glasfasernetze (FttB/H) ausbauen. Dafür investieren die Mitgliedsunternehmen des BREKO in jedem Jahr weit über 3 Mrd. Euro.

Für die BREKO-Mitgliedsunternehmen haben die Netz- und IT-Sicherheit ebenso wie die Sicherheit der Daten ihrer Kunden einen hohen Stellenwert. Den im BREKO organiserten Netzbetreibern und Diensteanbietern ist bewusst, dass die IT- und Datensicherheit ein ganz wesentliches

Qualitätsmerkmal iher hochwertigen glasfaserbasierten Produkte ist. Entsprechend ernst nehmen die Unternehmen die gesetzlichen Anforderungen.

Dies vorausgeschickt kommentieren wir das vom BMI veröffentlichte Diskussionspapier wie folgt.

II. Vermeidung einer Mehrfachregulierung

1. Erhebliche Ausdehnung des Adressatenkreises

Durch die NIS-2-Richtlinie und ihre Umsetzung wird der Adressatenkreis des BSI-Gesetzes erheblich erweitert und ist nicht mehr auf die klassischen KRITIS-Betreiber beschränkt. Neben den „Betreibern kritischer Anlagen“ sind – in abgestufter Intensität – nunmehr auch *„besonders wichtige Einrichtungen“* (in der Terminologie der Richtlinie „wesentliche Einrichtungen“) und *„wichtige Einrichtungen“* zur Einhaltung bestimmter Sicherheitsstandards und der Umsetzung der entsprechenden Maßnahmen verpflichtet. Dabei wird der Telekommunikationssektor sehr weitgehend den „besonders wichtigen Einrichtungen“ zugeordnet. Bereits ab 50 Mitarbeitenden bzw. einem Jahresumsatz bzw. einer Jahresbilanzsumme ab € 10 Mio. gelten Telekommunikationsnetzbetreiber und Telekommmunikationsdiensteanbieter als *„besonders wichtige Einrichtungen“* mit den entsprechenden gesetzlichen Verpflichtungen. Telekommunikationsnetzbetreiber und -Dienstanbieter unterhalb dieser Schwellwerte sind als Angehörige eines *„Sektors mit hoher Kritikalität“* (Anlage1, Ziffer 6) den für *„wichtige Einrichtungen“* geltenden Verpflichtungen unterworfen. Die Telekommunikationswirtschaft ist damit praktisch vollständig – und zum großen Teil erstmals – im Zuge der NIS-2-Umsetzung durch das im Zuge der Richtlinienumsetzung zur Neufassung anstehende BSI-Gesetz betroffen.

Die sich hieraus ergebenden Verpflichtungen können gerade von kleineren Telekommunikationsunternehmen (TKU) überhaupt nur dann bewältigt werden, wenn eine Mehrfachregulierung konsequent vermieden wird. Dies ist im Diskussionspapier aber nicht durchgehend sichergestellt. Zudem kann der Umstand, dass viele TK-Netzbetreiber und -Diensteanbieter erstmals durch das BSI-Gesetz verpflichtet werden nicht ohne Rückwirkungen auf die Umsetzungsfristen bleiben.

2. Bereichsausnahmen

Um eine Mehrfachregulierung zu verhindern, sieht § 28 Abs.4 Nr.1 BSIG-E weitgehende Bereichsausnahmen für die Telekommunikationswirtschaft vor. Danach sollen *„wichtige Einrichtungen“* und *„besonders wichtige Einrichtungen“* soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen von den Verpflichtungen nach §§ 30und 31 BSIG-E befreit sein.
Im Fall der Verpflichtung zur Umsetzung von Risikomanagementmaßnahmen nach § 30 TKG macht diese Bereichsausnahme Sinn, weil bereits durch den **Pflichtenkatalog nach § 165 TKG** in Verbindung mit dem **Sicherheitskataloig der BNetzA nach § 167 TKG** ein adäquat hohes Schutzniveau sichergestellt ist. Hier gilt der Vorrang der spezielleren sektorspezifischen Regelung.

Keinen Sinn macht allerdings die Bereichsausnahme mit Blick auf § 31 TKG, da dort nur spezielle Verpfichtungen für *„Betreiber kritischer Anlagen“* festgelegt werden, also *„wichtige Einrichtungen“* und *„besonders wichtige Einrichtungen“* (soweit es sich nicht um *„kritische Anlagen*“ handelt) gar nicht adressiert werden. Wir gehen davon aus, dass es sich insoweit um ein redaktionelles Versehen handelt und tatsächlich eine Bereichsausnahme in § 28 Abs.4 Nr.1 TKG für die Meldepflichten bei Sicherheitsvorfällen nach § 32 TKG statuiert werden sollte. Diesbezüglich ist eine Bereichsausnahme für „*wichtige Einrichtungen*“ und „*besonders wichtige Einrichtungen“* tatsächlich sinnvoll und notwendig, da bereits **§ 168 TKG** bei Vorliegen eines Sicherheitsvorfalls mit beträchtlichen Auswirkungen TK-Netzbetreibern und -Diensteanietern **bereits umfangreiche Mitteilungspflichten an die BNetzA und das BSI auferlegt** und somit ein vergleichbares Schutzniveau schafft. Eine zusätzliche Verpflichtung nach § 32 BSIG-E würde damit zu einer **unzulässigen Doppelregulierung** führen. Wir gehen daher davon aus, dass in § 28 Abs.4 Nr.1 BSIG-E keine Ausnahme von den Verpflichtungen des (hinsichtlich *„wichtigen Eirichtungen“* und „*besonders wichtigen Einrichtungen*“ ohnehin irrelevanten) § 31 BSIG-E, sondern eine Ausnahme von der Meldepflicht nach § 32 BSIG-E adressiert werden sollte.

Im Übrigen sieht das geltende BSIG in § 8d Abs.2 eine weitere Bereichsausnahme für Betreiber kritischer Infrastrukturen vor, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Dies betrifft u.a. den Einsatz von **Systemen der Angriffserkennung**. Diese Bereichsausnahme war auch schlüssig, da der Einsatz von

Systemen der Angriffserkennung für die Telekommunikationsbranche **bereits in § 165 Abs.3 TKG geregelt** wird. Das Diskussionspapier des BMI sieht aber nunmehr für „*Betreiber kritischer Anlagen*“ allgemein in § 31 TKG eine entsprechende Verpflichtung vor, ohne dass „Betreiber kritischer Anlagen“ im Bereich der Telekommunikation hiervon ausgenommen wären, so dass diesbezüglich die geltende Bereichsausnahme abgeschafft würde und eine Doppelung der Verpflichtung bestünde. Wir bitten das BMI daher darum, dieen Punkt noch einmal kritisch zu prüfen.

III. Geschäftsführerhaftung

Das Diskussionspapier sieht in § 38 BSIG-E eine umfangreiche Haftung der Geschäftsleiter *„besonders wichtiger Einrichtungen“* und „*wichtiger Einrichtungen“* im Hinblick auf die Umsetzung und Überwachung der gebotenen Risikomanagementmaßnahmen vor. Die Verantwortlichkeit kann weder horizontal z.B. im Vorstand noch vertikal auf einzelne Mitarbeitende komplett abdelegiert werden. Darüber hinaus besteht eine Verpflichtung der Geschäftsleiter zur Teilnahme an Schulungen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung von Risiken sowie Risikomanagementmaßnahmen im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Über diese bereits strengen Anforderungen aus Art. 20 der NIS-2-Richtlinie hinaus, sieht die geplante nationale Regelung in § 38 BSIG-E vor, dass ein Verzicht der Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung aufgrund einer Pflichtverletzung der Umsetzungs- und Überwachungspflicht zu Risikomanagementmaßnahmen oder ein Vergleich unwirksam sein sollen. Dies gilt jedenfalls bis zur Grenze der Abwendung eines Insolvenzverfahrens des Ersatzpflichtigen.

Der BREKO hält diese durch die umzusetzende Richtlinie nicht vorgebene Haftungsverschärfung für nicht angemessen. Die Geschäftsleitung würde dadurch einem **außerordentlich hohem und nicht verhältnismäßigen Risiko** ausgesetzt. Die strenge Haftungsregelung in Art.20 der NIS-2-Richtlinie ist unseres Erachtens vollkommen ausreichend, um den hohen Stellenwert der Cybersicherheitsanforderungen auch gegenüber der Geschäftsleitung abzusichern. Dazu kommt die intrinsische Motivation, den Kundinnen und Kunden auch in Bezug auf die IT- und Datensicherheit ein hochqualitatives Produkt anzubieten.

Wir regen daher an, **§ 38 Abs.2 BSIG-E zu streichen**. Zumindestens sollte aber klargestellt werden, dass die Inanspruchnahme einer entsprechenden Versicherung (D&O-Versicherung) zur Absicherung der Geschäftsleitung durch § 38 Abs.2 BSIG-E nicht ausgeschlossen werden soll.

IV. Übergangsregelungen

Artikel 29 des Diskussionspapiers sieht ein Inkrafttrten des neuen BSIG zum 1.10.2024 vor. In der Begründung zu Artikel 29 wird dazu ausgeführt, dass bei einem erwarteten Abschluss des Gesetzgebungsverfahrens im März 2024 den Unternehmen noch 6 Monate zur Verfügung stünden, um die notwenigen Maßnahmen zur Umetzung zu treffen. Diese Prämisse hält der BREKO in mehrfacher Hinsicht für fragwürdig.

Zum einen haben wir, angesichts der Tatsache, dass Ende Oktober 2023 noch nicht einmal ein Referentenentwurf, sondern lediglich ein Diskussionspapier vorliegt, erhebliche Zweifel daran, dass das Gesetzgebungsverfahren bis zum März b2024 bgeschlossen werden kann. Dies gilt insbesondere im Hinblick darauf, dass das neue BSIG nicht nur die im Diskussionspapier dargelegten Verpflichtungen für die Unternehmen regeln soll, sondern auch Verpflichtungen von staatlichen Stellen beinhaltet, so dass sicher erheblicher Diskussionsbedarf zwischen den beteiligten Ministerien, aber auch mit anderen öffentlichen Institutionen besteht.

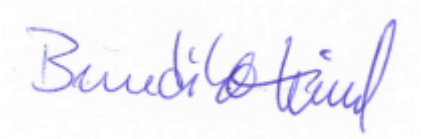
Zum anderen halten wir einenUmsetzungszeitraum von (bestenfalls) 6 Monaten für erheblich zu kurz, angesichts der Tatsache, dass die Verpflichtungen aus dem neuem BSIG durch die erhebliche Ausweitung des Adressatenkreises viele - und gerade kleinere - Unternehmen miit überschaubaren Ressourcen erstmals trifft.

Zwar ist es richtig, dass die von den Bereichsausnahmen umfassten Verpflichtungen durch das TKG vorgegeben sind und bereits seit Längerem umgesetzt sind. Das neue BSIG enthält aber auch eine Reihe darüber hinausgehender Verpflichtungen, die von den Unternehmen umgesetzt werden müssen. Erschwerend hinzu kommt, dass erst mit der nach § 57 BSIG-E ebenfalls zu erlassenden Verordnung hinreichend sicher klargestellt ist, welchem Adressatenkreis das betreffende Unternehmen zuzuordnen ist und welche Verpflichtungen genau umzusetzen sind.

Vor diesem Hinterurnd halten wir einen **Umsetzungszeitraum von mindestens 12 Monaten** nach Inkrafttreten des vollständigen Regelungswerks, einschließlich der Verordnung nach § 57 BSIG-E, für erforderlich.

Wir freuen uns auf eine vertiefte Erlörterung im Rahmen des vom BMI angebotenen Werkstattgesprächs am 26.10., stehen aber für Rückfragen gerne auch schon vorher zur Verfügung.

Mit freundlichen Grüßen



Benedikt Kind
Leiter Recht & Grundsatzfragen Regulierung